Information Sharing Agreement for Oxfordshire Safeguarding Children Board

Document Control	
Document version	2.0
Document owner	Oxfordshire Safeguarding Children Board (OSCB)
Document primary contact	oscb@oxfordshire.gov.uk Information.management@oxfordshire.gov.uk
Parties to this agreement	[Oxfordshire Safeguarding Children Board, Thames Valley Police, Oxfordshire Clinical Commissioning Group, Oxfordshire County Council, Oxford Health NHS Foundation Trust, Oxford University Hospitals, Cherwell District Council, Oxford City Council, South and Vale District Council, West Oxfordshire District Council, CAFCASS, National Probation Service, Thames Valley Community Rehabilitation Company, Schools, Housing Representative, Voluntary and Community Sector Representatives, Lay member Representatives]
Dates in force including review schedule	Date agreed: 30.09.20 Review date: 30.09.21

Once the party has signed at Annex A and completed Annex B please return copy to:

oscb@oxfordshire.gov.uk

&

information.management@oxfordshire.gov.uk

Part One

1. Introduction

i. Oxfordshire Safeguarding Children Board (OSCB) and its partner agencies ("the parties") are committed to maintaining safeguarding for children across Oxfordshire and will work together and exchange necessary information to achieve this.

ii. The parties to this agreement consist of public authorities and partners, including but not limited to Thames Valley Police, Oxfordshire County Council, Cherwell District Council, Oxford City Council, South Oxfordshire and Vale of White Horse District Councils, West Oxfordshire District Council, Oxfordshire Clinical Commissioning Group, Oxford University Hospitals, Oxford Health, probation and community rehabilitation services, along with schools and lay members. The OSCB membership can be viewed at: https://www.oscb.org.uk/about-us/board-membership

iii. It is the responsibility of these parties to ensure that they:

- adhere to the Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR) and all applicable legislative requirements, guidance and codes of practice for privacy and the processing of personal data;
- have a process by which the flow of information can be controlled;
- provide appropriate training on privacy and data protection;
- have adequate arrangements to monitor and maintain compliance with this agreement;
- maintain relevant professional and ethical standards.

iv. This document consists of two parts. Part One provides the overarching agreement of principles in sharing information for the purpose of safeguarding children. Part Two annexes the procedural form for doing so (Annex B) and supporting information.

2. Purpose and lawful basis for sharing

i. This agreement sets out the framework for the sharing of personal data between the parties as Data Controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

ii. In scope this agreement covers the sharing between the parties of any personal and sensitive data about persons and activities with the objective of safeguarding children, whether urgent or imminent, reactive or proactive, immediate or ongoing.

iii. The purpose for sharing this information is to ensure the parties can meet their statutory obligations to safeguard children, maintaining up to date, accurate, relevant records for identifying, actioning and monitoring safeguarding requirements and activities and outcomes.

iv. This agreement is in place to inform the reasons and methods of sharing for the purposes of safeguarding. Sharing for other purposes and other information is not covered by this agreement.

v. Data can only be used for the purpose shared and cannot be shared to third parties except where the purposes of this agreement apply, i.e. for the urgent intervention of safeguarding, risk of harm, or overriding safety requirement.

vi. Information shared may be personal data (GDPR Article 5) and may include special category data (GDPR Article 9 of GDPR). See Annex B.

vii. Such personal sensitive information must be shared, processed and stored securely and with suitable security classification. This requires the use of encrypted or secure email, secure password-protected end-user devices, discrete line of business systems, access controls, secure storage, appropriate audit functions, and "Official – Sensitive" classification markings.

viii. The lawful bases for sharing information between the Parties have been identified as:

- Legal obligation – processing is necessary to comply with a law or statutory duty
- Vital interest – processing is necessary to protect someone's life;
- Public interest – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the parties;
- Contract – processing is necessary for the fulfilment of a contract with the individual or to enter into a contract;
- Consent – the individual has freely given clear unambiguous consent to process their personal data;
- Law enforcement under Part 3 of the Data Protection Act 2018
- Safeguarding criteria under Schedule 1 Part 2 Paragraph 18 of the Data Protection Act 2018.

ix. The principle legislative instruments and codes of practice that provide for lawful sharing for safeguarding under this agreement are:

- Childrens' Acts 2004
- Care Act 2014
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Freedom of Information Act 2000
- Caldicott Principles (as revised)

- Common Law Duty of Confidentiality
- Code of practice on the Management of Police Information (MoPI) 2005 - 4.8. Sharing of police information outside the UK police service.
- Human Rights Act 1998

x. There are other pieces of legislation that place powers or duties to share information on public authorities and their partners. This list is not exhaustive. All information sharing must be in accordance with one or more presented lawful basis and legal power/duty.

3. Breaches, complaints, information requests and indemnity

i. In the event of a personal data breach or breach of confidentiality the parties will notify the relevant Data Controller as soon as possible and within 24 hours to enable the Data Controller to meet their responsibility to notify the ICO of a serious breach within 72 hours of becoming aware of the breach.

ii. In the event of a complaint, or a regulatory request, each party will provide the other will all reasonable assistance to answer that complaint or request within the timeframes permitted.

iii. In the event of a data subject request or Freedom of Information request being received by a party, the other parties will provide all reasonable assistance to one another to fulfil these requests within the timeframes permitted.

iv. Each party fully indemnifies the other against any and all costs, expenses and claims arising from any breach of this agreement by their employees, agents, contractors or data processors, and in particular, but without limitation, the unauthorised or unlawful loss, theft, use, destruction or disclosure by the offending party, its employees, agents, contractors or data processors, of any data obtained in connection with this agreement.

4. Review, training, assurance, publication and termination

i. The parties will review this agreement annually or upon any substantive change to the data, processing, legislation or parties of this agreement.

ii. The parties will ensure that all relevant staff are aware of this agreement and have adequate data protection training to work accordingly.

iii. The parties will provide all reasonable assurance to each other upon written request of their privacy and security arrangements to undertake the sharing and processing of data under this agreement.

iv. Each party will provide a single point of contact for the purpose of managing this agreement and ensuring that sharing is necessary, proportionate and lawful.

v. For public assurance and transparency this agreement will be published on the OSCB website.

vi. This agreement may also be published on the parties' external websites for the purpose of transparency and internal websites for the purpose of reference and training for staff.

vii. Any party may withdraw from this agreement at any time provided they give a minimum of 30 days' notice in writing to the other parties. Therewith they will be unable to share information and will be required to dispose of information in accordance with their retention policies.

viii. The obligations of confidentiality imposed on the parties by this agreement shall continue in force after the expiry or termination of this agreement.

Part 2

Annex A – The parties to this agreement

Each party to provide a named individual and role, along with signature and date, and the organisation's role of Data Controller or Processor.

Organisation (and Service or Department where applicable)	*e.g. Oxfordshire County Council Children's Services*
Data Controller or Data Processor?	*e.g. Data Controller*
Signatory for organisation (name, role and date)	*e.g. Kevin Gordon, Director of Children's Services, 01/01/2021*
Point of contact for agreement (name, role, email)	*e.g. OCC Information Management Team information.management@oxfordshire.gov.uk*

Organisation (and Service or Department where applicable)	*e.g. Thames Valley Police*
Data Controller or Data Processor?	*e.g. Data Controller*
Signatory for organisation (name, role and date)	*e.g. Chief Constable John Campbell, 01/01/2020*
Point of contact for agreement (name, role, email)	*e.g. Joint Information Management Unit*

Annex B – Procedure for sharing information

This annex should be completed by each party and returned with the signed agreement (Annex A). In this section, state the routine sharing undertaken for safeguarding. This annex may be repeated for any specific short-term share or thematic project undertaken with by OSCB parties under this agreement.

1. What will be shared? Detail the personal data and special category data involved. (Special category data is defined as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic/biometric identification data, health data, sex life or sexual orientation.)
Write here…

2. Where will it be shared? Describe the dataflow, with which organisation(s) and whether one-way or reciprocal?
Write here…

3. How will it be shared? Detail the methods of sharing, including emails, online forms/portals, data transfers or downloads, documents, spreadsheets, databases.
Write here…

4. How will it be secured? Detail the methods of secure transmission, receipt, storage and processing of the data, including secure email, devices and systems.
Write here…

5. How will it be processed and destroyed? Describe what the data will be used for, where it will be kept, and how long it will be kept for before being disposed of.
Write here…

6. Limitations on processing? Detail any limitations imposed on processing of the data that you share, e.g. only for health or policing purposes, or no onward sharing.
Write here…

7. What is the lawful basis? The purpose of information sharing under this agreement is safeguarding. Give your lawful basis and legislative instruments (as per Part One).
Write here…

8. Undertaking to share under the agreement:
Your organisation/service: *Write here*
Your OSCB member/authorising officer (name and role): *Write here*
Your point of contact (name and role): *Write here*

Appendix C: Good practice guidance
The following principles and checklist should be considered before processing or sharing of information occurs.

The Data Protection Principles

- Lawfulness, fairness and transparency – data processing must comply with the law, be fair to data subjects involved and made clear via a privacy statement or notice.
- Purpose limitation – data processed must be for a specific purpose, clearly stated, and only for as long as necessary to complete that purpose.
- Data minimisation – only the data needed for the purposes should be processed. This makes it easier to protect and easier to keep up to date and accurate.
- Accuracy – data should be kept accurate and every reasonable step must be taken to erase or rectify data that is inaccurate or incomplete.
- Storage limitation – data should be deleted when no longer required.
- Integrity and confidentiality – data must be processed with appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Caldicott Principles

- Justify the purpose(s) for using confidential information.
- Do not use personal confidential data unless it is absolutely necessary.
- Use the minimum necessary personal confidential data.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

Checklist for information processing and sharing

- We know the identity, organisation and role of the parties sharing.
- We know the reason the information is required and have documented the purpose and lawful basis for processing and sharing.
- We are fully satisfied that it is necessary to share in full, and we could not achieve the objective without sharing or by using anonymised data.
- We have understood the risks posed to an individual's privacy or safety.
- We are not sharing more information than is necessary.
- We have ensured that the information is being shared securely.
- Where special category data is involved, we have identified a condition for processing it and documented this.
- Where criminal offence data is involved, we have identified a condition for processing it and documented this.
- We have established whether this is a one-off, periodic or routine sharing.
- We have been clear with the parties how the information will be used, and it is covered within our privacy notice or policy.
- We will inform the parties if any of the information is potentially inaccurate or unreliable.
- Where we consider using consent to lawfully share information, we will respect the individual's wishes and withdrawal of consent.
- Check with a manager/specialist or seek legal advice if you are unsure.